15

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001184789 A**

(43) Date of publication of application: **06.07.01**

(51) Int. Cl **G11B 20/10**
G06F 12/14
G09C 5/00
H04L 9/32

(21) Application number: **11366074**

(22) Date of filing: **24.12.99**

(71) Applicant: **TAIYO YUDEN CO LTD**

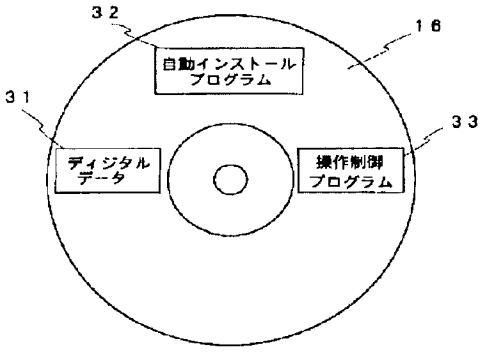
(72) Inventor: **OMURA YUKIHIDE**
SUNAKAWA RYUICHI

(54) **OPTICAL INFORMATION RECORDING MEDIUM, METHOD AND SYSTEM FOR HOLDING INFORMATION SECRECY**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an optical information recording medium, a method and a system for holding information secrecy, with which the illegal use or the like of recorded information can be prevented.

SOLUTION: When recording information on a CD-R 16, in addition to digital data 31, an automatic install program 32 and an operation control program 33 are written together. When the CD-R 16 is loaded into an information reproducing device, the automatic install program 32 is automatically started and the operation control program is made resident and started in the memory of the information reproducing device. When operation to digital data written on the CD-R 16 is detected, the operation control program 33 calls the entry of a password by interrupting this operation and when the inputted password is a regular password, interrupted operation is continued.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－184789
（P2001－184789A）
(43)公開日　平成13年７月６日(2001.7.6)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｃ１１Ｂ　20/10	Ｈ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｃ０６Ｆ　12/14	３２０Ｅ	５Ｄ０４４
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00		５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	９Ａ００１
			６７３Ｃ	

審査請求　未請求　請求項の数21　ＯＬ　（全 14 頁）

(21)出願番号　特願平11－366074

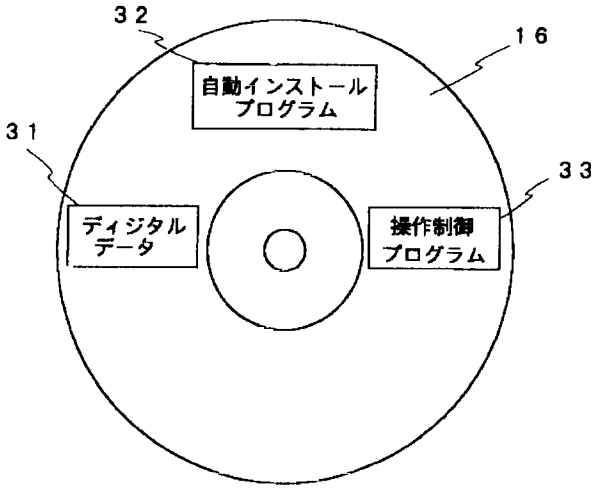
(22)出願日　平成11年12月24日(1999.12.24)

(71)出願人　000204284
太陽誘電株式会社
東京都台東区上野６丁目16番20号
(72)発明者　大村　幸秀
東京都台東区上野６丁目16番20号　太陽誘電株式会社内
(72)発明者　砂川　隆一
東京都台東区上野６丁目16番20号　太陽誘電株式会社内
(74)代理人　100069981
弁理士　吉田　精孝　（外１名）

最終頁に続く

(54)【発明の名称】　光情報記録媒体並びに情報機密保持方法及びそのシステム

(57)【要約】
【課題】　記録情報の不正使用等を防止できる光情報記録媒体並びに情報機密保持方法及びそのシステムを提供する。
【解決手段】　情報をＣＤ－Ｒ１６に記録する際に、ディジタルデータ３１に加えて、自動インストールプログラム３２と操作制御プログラム３３を一緒に書き込む。自動インストールプログラム３２は、ＣＤ－Ｒ１６を情報再生装置へ装填したときに自動的に起動して操作制御プログラムを情報再生装置のメモリに常駐起動させ、操作制御プログラム３３はＣＤ－Ｒ１６内に書き込まれているディジタルデータへの操作を検出したときに、この操作を中断させパスワードの入力を促し、入力されたパスワードが正規のパスワードであるときに中断していた操作を継続させる処理を行う。



【特許請求の範囲】

【請求項１】　ディジタルデータと、
前記ディジタルデータへの操作を検出したときに該操作を中断させパスワードの入力を促し、入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う第１のコンピュータプログラムと、
少なくともメモリに常駐するコンピュータプログラムを動作させる情報再生装置への装填時に、自動的に起動して前記第１のコンピュータプログラムを前記情報再生装置のメモリに常駐させる第２のコンピュータプログラムとが記録されていることを特徴とする光情報記録媒体。

【請求項２】　前記ディジタルデータは、基本データに対して電子透かしデータが埋め込まれたディジタルデータであることを特徴とする請求項１記載の光情報記録媒体。

【請求項３】　前記ディジタルデータは、基本データに対して電子透かしデータを埋め込んだデータをさらに暗号化したディジタルデータであることを特徴とする請求項１記載の光情報記録媒体。

【請求項４】　前記ディジタルデータは、基本データに対して電子透かしデータが埋め込まれたディジタルデータであり、
前記第１のコンピュータプログラムは、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段を含んでいることを特徴とする請求項１記載の光情報記録媒体。

【請求項５】　前記ディジタルデータは、基本データに対して電子透かしデータを埋め込んだデータをさらに暗号化したディジタルデータであり、
前記第１のコンピュータプログラムは、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータを復号してから前記電子透かしデータを除去して前記基本データを取り出す手段を含んでいることを特徴とする請求項１記載の光情報記録媒体。

【請求項６】　前記第１のコンピュータプログラムは、検出対象とする前記ディジタルデータへの操作の１つとして、前記ディジタルデータの複写操作を含んでいることを特徴とする請求項１記載の光情報記録媒体。

【請求項７】　追記型の光情報記録媒体であることを特徴とする請求項１記載の光情報記録媒体。

【請求項８】　前記ディジタルデータは、基本データに対して電子透かしデータが埋め込まれ且つ該電子透かしデータの一部に前記正規のパスワードが含まれているディジタルデータであり、
前記第１のコンピュータプログラムは、前記電子透かしデータから前記正規のパスワードを抽出する手段と、該抽出した正規のパスワードと前記入力されたパスワードとを比較する手段とを含んでいることを特徴とする請求項１記載の光情報記録媒体。

【請求項９】　光情報記録媒体に情報を書き込み、少なくともメモリに常駐するコンピュータプログラムを動作させる情報再生装置を用いて前記情報が書き込まれている光情報記録媒体から前記情報を取り出して利用するときの情報機密保持方法であって、
前記光情報記録媒体に対して前記情報を書き込むときに、
前記情報に基づくディジタルデータと、
該ディジタルデータへの操作を検出したときに該操作を中断させパスワードの入力を促すと共に入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う第１のコンピュータプログラムと、
前記情報再生装置への装填時に、自動的に起動して前記第１のコンピュータプログラムを前記情報再生装置のメモリに常駐させる第２のコンピュータプログラムとを前記光情報記録媒体に書き込むことを特徴とする情報機密保持方法。

【請求項１０】　前記光情報記録媒体に対して前記情報を書き込むときに、
前記情報をデータ化した基本データに対して電子透かしデータを埋め込んで前記ディジタルデータを生成し、
前記第１のコンピュータプログラムを、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものとすることを特徴とする請求項９記載の情報機密保持方法。

【請求項１１】　前記光情報記録媒体に対して前記情報を書き込むときに、
前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだデータを生成した後、さらに該データを暗号化して前記ディジタルデータを生成し、
前記第１のコンピュータプログラムを、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータを復号してから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものとすることを特徴とする請求項９記載の情報機密保持方法。

【請求項１２】　前記第１のコンピュータプログラムを、検出対象とする前記ディジタルデータへの操作の１つとして前記ディジタルデータの複写操作を含んだものとすることを特徴とする請求項９記載の情報機密保持方法。

【請求項１３】　前記光情報記録媒体として追記型の光情報記録媒体を用いることを特徴とする請求項９記載の情報機密保持方法。

【請求項１４】　前記光情報記録媒体に対して前記情報

を書き込むときに、
前記情報をデータ化した基本データに対して前記正規のパスワードのデータを含む電子透かしデータを埋め込んで前記ディジタルデータを生成し、
前記第１のコンピュータプログラムを、前記電子透かしデータから前記正規のパスワードを抽出する手段と、該抽出した正規のパスワードと前記入力されたパスワードとを比較する手段とを含んだものとすることを特徴とする請求項９記載の情報機密保持方法。
【請求項１５】　情報記録装置を用いて光情報記録媒体に情報を書き込み、少なくともメモリに常駐するコンピュータプログラムを動作させる情報再生装置を用いて前記情報が書き込まれている光情報記録媒体から前記情報を取り出して利用する情報機密保持システムであって、
前記情報記録装置は、
機密保持対象となるディジタルデータへの操作を検出したときに該操作を中断させパスワードの入力を促すと共に入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う第１のコンピュータプログラムを保持する手段と、
前記情報再生装置への装填時に自動的に起動して前記第１のコンピュータプログラムを前記情報再生装置のメモリに常駐させる第２のコンピュータプログラムを保持する手段と、
前記光情報記録媒体に対して前記情報を書き込むときに、前記情報に基づくディジタルデータと共に前記第１のコンピュータプログラムと前記第２のコンピュータプログラムとを前記光情報記録媒体に書き込む手段を備えていることを特徴とする情報機密保持システム。
【請求項１６】　前記第１のコンピュータプログラムは、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものであり、
前記情報記録装置は、
前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んで前記ディジタルデータを生成する手段を備えていることを特徴とする請求項１５記載の情報機密保持システム。
【請求項１７】　前記第１のコンピュータプログラムは、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータを復号してから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものであり、
前記情報記録装置は、
前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだデータを生成する手段と、　該電子透かしデータが埋め込まれたデータを暗号化して前記ディジタルデータを生成する手段とを備えていることを特徴とする請求項１５記載の情報機密保持システム。
【請求項１８】　前記第１のコンピュータプログラムは、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータを復号する外部プログラムを動作させて復号されたディジタルデータを得る手段と、該復号されたディジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段とを含んだものであり、
前記情報記録装置は、
前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだデータを生成する手段と、
該電子透かしデータが埋め込まれたデータを暗号化して前記ディジタルデータを生成する手段とを備え、
前記情報再生装置は、前記暗号化されたディジタルデータを復号するコンピュータプログラムを前記外部プログラムとして備えていることを特徴とする請求項１５記載の情報機密保持システム。
【請求項１９】　前記第１のコンピュータプログラムは、検出対象とする前記ディジタルデータへの操作の１つとして前記ディジタルデータの複写操作を含んだものであることを特徴とする請求項１５記載の情報機密保持システム。
【請求項２０】　前記光情報記録媒体が追記型の光情報記録媒体であることを特徴とする請求項１５記載の情報機密保持システム。
【請求項２１】　前記第１のコンピュータプログラムは、前記電子透かしデータから前記正規のパスワードを抽出する手段と、該抽出した正規のパスワードと前記入力されたパスワードとを比較する手段とを含んだものであり、
前記情報記録装置は、
前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して前記正規のパスワードのデータを含む電子透かしデータを埋め込んで前記ディジタルデータを生成する手段を備えていることを特徴とする請求項１５記載の情報機密保持システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報機密保持能力を向上させた光情報記録媒体及び情報機密保持方法及びそのシステムに関するものである。
【０００２】
【従来の技術】近年、パーソナルコンピュータやオーディオ・ビジュアル機器を含む各種の電子機器発達が目覚ましく、高性能で低価格のこの種の商品が普及するようになった。これに伴い、パーソナルコンピュータやオーディオ・ビジュアル機器にて使用するディジタルデータ

も多種に亘り、ディジタルデータ等のソフト商品の販売や流通も盛んになっている。

【０００３】一方、事務処理等もコンピュータを用いて行うことがほとんどであり、扱うディジタルデータの量も膨大な量となってきている。このため、万一に備えてＣＤ－Ｒなどの情報記録媒体にデータのバックアップを取っておくことも一般的に行われている。

【０００４】このような状況下において、コンピュータを扱える人の数は急増し、ディジタルデータのコピーも容易に行えることから、オリジナルのディジタルデータをコピーした複製を不正に作成して、それを他人に再配布したり、或いは機密保持を有する情報が漏洩してしまう可能性がある。

【０００５】これらの不正使用を防止するために、データの暗号化技術や一般的に電子透かしと呼ばれる技術が研究されている。

【０００６】データの暗号化とは、主としてコンピュータネットワークにおいて複数の人物がデータをやりとりする時に、データそのものを守るために開発されてきた技術で、悪意のある第三者がデータを取得して使用したり或いは改ざんしたりすることを防止するために用いられている。

【０００７】この暗号化技術を用いると、暗号化されたデータはこのデータをやりとりする人間にしか解読できないようになり、第三者がデータを取得してもその内容を解読することはできない。

【０００８】この暗号化技術としては、暗号化データを復号するときにもデータを暗号化したときの暗号鍵を共通に用いる共通鍵方式と、暗号化するための鍵を公開鍵として他者に対して公開しておき、復号化のための鍵を個人鍵として自分自身の手元に保管しておく公開鍵方式が、一般的に広く用いられている。

【０００９】電子透かしとは、オリジナルのディジタルデータにある操作を加え、ディジタルデータに関する情報を、ディジタルデータ自体に埋め込む技術である。この技術を応用することによって、例えば、不正コピーが発見された場合に、誰がその不正コピーを再配布したのかを特定することも可能である。また、電子透かしの技術を実現する方法としては、現在、離散コサイン変換、フーリエ変換、ウェーブレット変換等を用いた方法が研究されている。

【００１０】

【発明が解決しようとする課題】しかしながら、暗号化技術や電子透かし技術を用いて加工したディジタルデータであっても、他の情報記録媒体に不正にコピーすることは可能である。これを防止するためには、情報記録媒体への情報記録装置或いは情報再生装置又は双方の機能を備えた情報記録再生装置に不正コピーを防止するための特殊な機能を設ける必要があるが、未だ実現に至っていない。

【００１１】本発明の目的は上記の問題点に鑑み、記録情報の不正使用等を防止できる光情報記録媒体並びに情報機密保持方法及びそのシステムを提供することである。

【００１２】

【課題を解決するための手段】本発明は上記の目的を達成するために請求項１では、ディジタルデータと、前記ディジタルデータへの操作を検出したときに該操作を中断させパスワードの入力を促し、入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う第１のコンピュータプログラムと、少なくともメモリに常駐するコンピュータプログラムを動作させる情報再生装置への装填時に、自動的に起動して前記第１のコンピュータプログラムを前記情報再生装置のメモリに常駐させる第２のコンピュータプログラムとが記録されている光情報記録媒体を提案する。

【００１３】該光情報記録媒体内に書き込まれている情報を読み出す等の操作を行うために、該光情報記録媒体を情報再生装置に装填すると、自動的に前記第２のコンピュータプログラムが起動して前記第１のコンピュータプログラムを前記情報再生装置のメモリに常駐させる。これにより、前記第１のコンピュータプログラムは、前記情報再生装置内で動作し、前記光情報記録媒体に書き込まれている前記ディジタルデータに対する情報記録再生装置からの操作を監視する。この操作には、例えば前記ディジタルデータのコピー操作、前記ディジタルデータが文字情報や画像情報である場合はその表示操作、前記ディジタルデータがコンピュータプログラムである場合にはその実行操作、前記ディジタルデータが音声情報である場合はその再生操作等の何れであっても良い。さらに、前記情報再生装置内で動作する前記第１のコンピュータプログラムは、前記情報再生装置から前記ディジタルデータへの操作を検出したときに、該操作を中断させてパスワードの入力を促し、入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う。これにより、前記正規のパスワードを知らない者は前記光情報記録媒体内のディジタルデータを操作することができない。

【００１４】また、請求項２では、請求項１記載の光情報記録媒体において、前記ディジタルデータは、基本データに対して電子透かしデータが埋め込まれたディジタルデータである光情報記録媒体を提案する。

【００１５】該光情報記録媒体では、前記ディジタルデータは、書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれたデータである。これにより、正規パスワードを入力して前記ディジタルデータを操作しても、操作後のディジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。

【００１６】また、請求項３では、請求項１記載の光情報記録媒体において、前記ディジタルデータは、基本データに対して電子透かしデータを埋め込んだデータをさらに暗号化したディジタルデータである光情報記録媒体を提案する。

【００１７】該光情報記録媒体では、前記ディジタルデータは、書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれ、さらに暗号化されたデータである。これにより、正規パスワードを入力して前記ディジタルデータを操作しても、前記ディジタルデータを復号できなければ前記基本情報を得ることはできない。さらに、復号できても、復号後のディジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。

【００１８】また、請求項４では、請求項１記載の光情報記録媒体において、前記ディジタルデータは、基本データに対して電子透かしデータが埋め込まれたディジタルデータであり、前記第１のコンピュータプログラムは、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段を含んでいる光情報記録媒体を提案する。

【００１９】該光情報記録媒体では、前記ディジタルデータは、書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれたデータである。これにより、正規パスワードを入力して前記ディジタルデータを操作しても、操作後のディジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記ディジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【００２０】また、請求項５では、請求項１記載の光情報記録媒体において、前記ディジタルデータは、基本データに対して電子透かしデータを埋め込んだデータをさらに暗号化したディジタルデータであり、前記第１のコンピュータプログラムは、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータを復号してから前記電子透かしデータを除去して前記基本データを取り出す手段を含んでいる光情報記録媒体を提案する。

【００２１】該光情報記録媒体では、前記ディジタルデータは、書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれ、さらに暗号化されたデータである。これにより、正規パスワードを入力して前記ディジタルデータを操作しても、前記ディジタルデータを復号できなければ前記基本情報を得ることはできない。さらに、復号できても、復号後のディジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記ディジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【００２２】また、請求項６では、請求項１記載の光情報記録媒体において、前記第１のコンピュータプログラムは、検出対象とする前記ディジタルデータへの操作の１つとして、前記ディジタルデータの複写操作を含んでいる光情報記録媒体を提案する。

【００２３】該光情報記録媒体では、前記正規のパスワードを入力しなければ前記ディジタルデータを複写、即ちコピーすることができない。

【００２４】また、請求項７では、請求項１記載の光情報記録媒体において、追記型の光情報記録媒体である光情報記録媒体を提案する。

【００２５】該光情報記録媒体は追記型であるので、書き込まれている情報やコンピュータプログラムの改竄は全く不可能となる。

【００２６】また、請求項８では、請求項１記載の光情報記録媒体において、前記ディジタルデータは、基本データに対して電子透かしデータが埋め込まれ且つ該電子透かしデータの一部に前記正規のパスワードが含まれているディジタルデータであり、前記第１のコンピュータプログラムは、前記電子透かしデータから前記正規のパスワードを抽出する手段と、該抽出した正規のパスワードと前記入力されたパスワードとを比較する手段とを含んでいる光情報記録媒体を提案する。

【００２７】該光情報記録媒体では、前記電子透かしデータ内に前記正規のパスワードが含まれているため、正規のパスワードを知らない者が正規のパスワードを抽出することは困難になる。

【００２８】また、請求項９では、光情報記録媒体に情報を書き込み、少なくともメモリに常駐するコンピュータプログラムを動作させる情報再生装置を用いて前記情報が書き込まれている光情報記録媒体から前記情報を取り出して利用するときの情報機密保持方法であって、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報に基づくディジタルデータと、該ディジタルデータへの操作を検出したときに該操作を中断させパスワードの入力を促すと共に入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う第１のコンピュータプログラムと、前記情報再生装置への装填時に、自動的に起動して前記第１のコンピュータプログラムを前記情報再生装置のメモリに常駐させる第２のコンピュータプログラムとを前記光情報記録媒体に書き込む情報機密保持方法を提案する。

【００２９】該情報機密保持方法によれば、光情報記録媒体に対して前記情報を書き込むときに、前記情報に基づくディジタルデータと、前記第１及び第２のコンピュータプログラムが書き込まれるので、該光情報記録媒体内に書き込まれている情報を読み出す等の操作を行うために、該光情報記録媒体を情報再生装置に装填すると、自動的に前記第２のコンピュータプログラムが起動して前記第１のコンピュータプログラムを前記情報再生装置のメモリに常駐させる。これにより、前記第１のコンピュータプログラムは、前記情報再生装置内で動作し、前記光情報記録媒体に書き込まれている前記ディジタルデータに対する情報記録再生装置からの操作を監視する。この操作には、例えば前記ディジタルデータのコピー操作、前記ディジタルデータが文字情報や画像情報である場合はその表示操作、前記ディジタルデータがコンピュータプログラムである場合にはその実行操作、前記ディジタルデータが音声情報である場合はその再生操作等の何れであっても良い。さらに、前記情報再生装置内で動作する前記第１のコンピュータプログラムは、前記情報再生装置から前記ディジタルデータへの操作を検出したときに、該操作を中断させてパスワードの入力を促し、入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う。これにより、前記正規のパスワードを知らない者は前記光情報記録媒体内のディジタルデータを操作することができない。

【００３０】また、請求項１０では、請求項９記載の情報機密保持方法において、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んで前記ディジタルデータを生成し、前記第１のコンピュータプログラムを、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものとする情報機密保持方法を提案する。

【００３１】該情報機密保持方法によれば、書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれたデータが前記ディジタルデータとして光情報記録媒体に書き込まれる。これにより、正規パスワードを入力して前記ディジタルデータを操作しても、操作後のディジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記ディジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【００３２】また、請求項１１では、請求項９記載の情報機密保持方法において、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだデータを生成した後、さらに該データを暗号化して前記ディジタルデータを生成し、前記第１のコンピュータプログラムを、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータを復号してから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものとする情報機密保持方法を提案する。

【００３３】該情報機密保持方法によれば、書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれ、さらに暗号化されたデータが前記ディジタルデータとして光情報記録媒体に書き込まれる。これにより、正規パスワードを入力して前記ディジタルデータを操作しても、前記ディジタルデータを復号できなければ前記基本情報を得ることはできない。さらに、復号できても、復号後のディジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記ディジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【００３４】また、請求項１２では、請求項９記載の情報機密保持方法において、前記第１のコンピュータプログラムを、検出対象とする前記ディジタルデータへの操作の１つとして前記ディジタルデータの複写操作を含んだものとする情報機密保持方法を提案する。

【００３５】該情報機密保持方法によれば、前記正規のパスワードを入力しなければ前記ディジタルデータを複写即ちコピーすることができない。

【００３６】また、請求項１３では、請求項９記載の情報機密保持方法において、前記光情報記録媒体として追記型の光情報記録媒体を用いる情報機密保持方法を提案する。

【００３７】該情報機密保持方法によれば、前記光情報記録媒体が追記型であるので、書き込まれている情報やコンピュータプログラムの改竄は全く不可能となる。

【００３８】また、請求項１４では、請求項９記載の情報機密保持方法において、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して前記正規のパスワードのデータを含む電子透かしデータを埋め込んで前記ディジタルデータを生成し、前記第１のコンピュータプログラムを、前記電子透かしデータから前記正規のパスワードを抽出する手段と、該抽出した正規のパスワードと前記入力されたパスワードとを比較する手段とを含んだものとする情報機密保持方法を提案する。

【００３９】該情報機密保持方法によれば、前記電子透かしデータ内に前記正規のパスワードが含まれているた

め、正規のパスワードを知らない者が正規のパスワードを抽出することは困難になる。

【００４０】また、請求項１５では、情報記録装置を用いて光情報記録媒体に情報を書き込み、少なくともメモリに常駐するコンピュータプログラムを動作させる情報再生装置を用いて前記情報が書き込まれている光情報記録媒体から前記情報を取り出して利用する情報機密保持システムであって、前記情報記録装置は、機密保持対象となるディジタルデータへの操作を検出したときに該操作を中断させパスワードの入力を促すと共に入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う第１のコンピュータプログラムを保持する手段と、前記情報再生装置への装填時に自動的に起動して前記第１のコンピュータプログラムを前記情報再生装置のメモリに常駐させる第２のコンピュータプログラムを保持する手段と、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報に基づくディジタルデータと共に前記第１のコンピュータプログラムと前記第２のコンピュータプログラムとを前記光情報記録媒体に書き込む手段を備えている情報機密保持システムを提案する。

【００４１】該情報機密保持システムによれば、前記情報記録装置によって光情報記録媒体に対して前記情報を書き込むときに、前記情報に基づくディジタルデータと、前記第１及び第２のコンピュータプログラムが書き込まれるので、該光情報記録媒体内に書き込まれている情報を読み出す等の操作を行うために、該光情報記録媒体を情報再生装置に装填すると、自動的に前記第２のコンピュータプログラムが起動して前記第１のコンピュータプログラムを前記情報再生装置のメモリに常駐させる。これにより、前記第１のコンピュータプログラムは、前記情報再生装置内で動作し、前記光情報記録媒体に書き込まれている前記ディジタルデータに対する情報記録再生装置からの操作を監視する。この操作には、例えば前記ディジタルデータのコピー操作、前記ディジタルデータが文字情報や画像情報である場合はその表示操作、前記ディジタルデータがコンピュータプログラムである場合にはその実行操作、前記ディジタルデータが音声情報である場合はその再生操作等の何れであっても良い。さらに、前記情報再生装置内で動作する前記第１のコンピュータプログラムは、前記情報再生装置から前記ディジタルデータへの操作を検出したときに、該操作を中断させてパスワードの入力を促し、入力されたパスワードが正規のパスワードであるときに前記中断していた操作を継続させる処理を行う。これにより、前記正規のパスワードを知らない者は前記光情報記録媒体内のディジタルデータを操作することができない。

【００４２】また、請求項１６では、請求項１５記載の情報機密保持システムにおいて、前記第１のコンピュータプログラムは、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものであり、前記情報記録装置は、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んで前記ディジタルデータを生成する手段を備えている情報機密保持システムを提案する。

【００４３】該情報機密保持システムによれば、前記情報記録装置によって書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれたデータが前記ディジタルデータとして光情報記録媒体に書き込まれる。これにより、情報再生装置において正規パスワードを入力して前記ディジタルデータを操作しても、操作後のディジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記ディジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【００４４】また、請求項１７では、請求項１５記載の情報機密保持システムにおいて、前記第１のコンピュータプログラムは、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータを復号してから前記電子透かしデータを除去して前記基本データを取り出す手段を含んだものであり、前記情報記録装置は、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだデータを生成する手段と、　該電子透かしデータが埋め込まれたデータを暗号化して前記ディジタルデータを生成する手段とを備えている情報機密保持システムを提案する。

【００４５】該情報機密保持システムによれば、前記情報記録装置において書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれ、さらに暗号化されたデータが前記ディジタルデータとして光情報記録媒体に書き込まれる。これにより、前記情報再生装置において正規パスワードを入力して前記ディジタルデータを操作しても、前記ディジタルデータを復号できなければ前記基本情報を得ることはできない。さらに、復号できても、復号後のディジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記ディジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【００４６】また、請求項１８では、請求項１５記載の情報機密保持システムにおいて、前記第１のコンピュー

タプログラムは、前記ディジタルデータへの操作が前記基本データの読み出し操作であるときに、前記ディジタルデータを復号する外部プログラムを動作させて復号されたディジタルデータを得る手段と、該復号されたディジタルデータから前記電子透かしデータを除去して前記基本データを取り出す手段とを含んだものであり、前記情報記録装置は、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して電子透かしデータを埋め込んだデータを生成する手段と、該電子透かしデータが埋め込まれたデータを暗号化して前記ディジタルデータを生成する手段とを備え、前記情報再生装置は、前記暗号化されたディジタルデータを復号するコンピュータプログラムを前記外部プログラムとして備えている情報機密保持システムを提案する。

【００４７】該情報機密保持システムによれば、前記情報記録装置において書き込み対象となる基本情報に基づいた基本データに対して、前記基本情報とは異なる情報が電子透かしデータとして埋め込まれ、さらに暗号化されたデータが前記ディジタルデータとして光情報記録媒体に書き込まれる。これにより、前記情報再生装置において正規パスワードを入力して前記ディジタルデータを操作しても、前記ディジタルデータを復号できなければ前記基本情報を得ることはできない。また、前記情報再生装置に前記暗号化されたディジタルデータを復号するコンピュータプログラムが存在しなければ、前記暗号化されたディジタルデータを復号することはできない。さらに、前記暗号化データを復号できても、復号後のディジタルデータから前記電子透かしデータを抽出することによって前記基本情報とは異なる情報を得ることができる。また、基本データの読み出し操作であるときは、前記正規のパスワードを入力することにより前記ディジタルデータから前記電子透かしデータが除去された前記基本データを取り出すことができる。

【００４８】また、外部プログラムが、ＣＤ－ＲＯＭ、ＣＤ－Ｒ等でデータと共に配信される場合は、バージョンアップの際に互換性を考慮する必要が低くなる。また、ＣＤ－ＲＯＭ上の外部プログラムをＯＳ(Operating System)レベルで起動させるようにすれば、外部プログラムのコピーを困難にすることも可能である。

【００４９】また、請求項１９では、請求項１５記載の情報機密保持システムにおいて、前記第１のコンピュータプログラムは、検出対象とする前記ディジタルデータへの操作の１つとして前記ディジタルデータの複写操作を含んだものである情報機密保持システムを提案する。

【００５０】該情報機密保持システムによれば、前記正規のパスワードを入力しなければ前記ディジタルデータを複写即ちコピーすることができない。

【００５１】また、請求項２０では、請求項１５記載の情報機密保持システムにおいて、前記光情報記録媒体が追記型の光情報記録媒体である情報機密保持システムを提案する。

【００５２】該情報機密保持システムによれば、前記光情報記録媒体が追記型であるので、書き込まれている情報やコンピュータプログラムの改竄は全く不可能となる。

【００５３】また、請求項２１では、請求項１５記載の情報機密保持システムにおいて、前記第１のコンピュータプログラムは、前記電子透かしデータから前記正規のパスワードを抽出する手段と、該抽出した正規のパスワードと前記入力されたパスワードとを比較する手段とを含んだものであり、前記情報記録装置は、前記光情報記録媒体に対して前記情報を書き込むときに、前記情報をデータ化した基本データに対して前記正規のパスワードのデータを含む電子透かしデータを埋め込んで前記ディジタルデータを生成する手段を備えている情報機密保持システムを提案する。

【００５４】該情報機密保持システムによれば、前記電子透かしデータ内に前記正規のパスワードが含まれており、前記第１のコンピュータプログラムは該正規のパスワードを抽出して比較に用いているため、正規のパスワードを知らない者が正規のパスワードを抽出することは困難になる。

【００５５】

【発明の実施の形態】以下、図面に基づいて本発明の一実施形態を説明する。

【００５６】図１は、本発明の第１の実施形態における情報機密保持システムを示す外観図、図２はその電気系回路示すブロック図である。図において、１は情報機密保持システムで、パーソナルコンピュータ本体１１、モニター１２、キーボード１３、マウス１４、ＣＤ－Ｒライター１５及び一般的にＣＤ－Ｒと称されているライトワンス追記型光ディスク（以下、ＣＤ－Ｒと称する）１６から構成されている。

【００５７】パーソナルコンピュータ本体（以下、コンピュータ本体と称する）１１は、周知のＣＰＵ２１、メモリ２２、表示制御部２３、ハードディスク装置２４、フロッピーディスク装置２５、及びＣＤドライブ装置２６を備えている。

【００５８】ＣＰＵ２１には、表示制御部２３を介してモニター１２が接続されると共に、図示せぬインタフェースを介してキーボード１３、マウス１４及びＣＤ－Ｒライター１５が接続されている。

【００５９】ＣＰＵ２１は、ハードディスク装置２４に格納されているプログラムをメモリ２２内に読み込み或いはメモリに常駐させ、このメモリ２２内のプログラムによって動作する。また、ＣＰＵ２１は、表示制御部２３を介してモニター１２に情報の表示を行うと共に、キーボード１３及びマウス１４を介して入力されたデータ及び命令を読み込むと共にこれを実行する。さらに、Ｃ

ＰＵ２１は、ハードディスク装置２４内のデータをアクセスすると共に、フロッピーディスク装置２５及びＣＤドライブ装置に装填されたフロッピーディスク或いはＣＤ内のデータをアクセスする。

【００６０】ハードディスク装置２４には、各種のアプリケーションプログラムやデータが格納され、本願発明に係るアプリケーションプログラムとして、電子透かし埋め込みモジュール、ＣＤ－Ｒ記録モジュール、自動インストールプログラム、操作制御プログラム及び機密情報書き込みモジュールが格納されている。

【００６１】次に、上記のシステムを用いてＣＤ－Ｒ１６に機密情報を記録する際の操作及びＣＰＵ２１の動作を説明する。

【００６２】ＣＤ－Ｒ１６に機密情報を記録するときは、前述した機密情報書き込みモジュールを起動する。起動後、ＣＰＵ２１はこのモジュールのプログラムに従って図３に示す通り動作して情報の記録処理を行う。

【００６３】即ち、機密情報書き込みモジュールを起動すると、ＣＰＵ２１は、まずパスワードの設定画面を表示してパスワードの設定を促す（ＳＡ１）。このパスワードは操作者が任意に設定するもので、記録した情報を操作する際に使用するものである。

【００６４】次いで、ＣＰＵ２１は、記録対象となる情報のファイルの指定を促し、操作者によってファイルが指定されると、電子透かし埋め込みモジュールを起動して指定されたファイルのディジタルデータ（基本データ）に対して電子透かしデータを埋め込んだディジタルデータを生成する（ＳＡ２）。このとき、電子透かしデータの一部に、前記ＳＡ１の処理で設定されたパスワードが正規パスワードとして埋め込まれる。また、パスワード以外の電子透かしデータは、電子透かし埋め込みモジュールを起動することによって任意に設定可能になっている。

【００６５】この後、ＣＰＵ２１は、ＣＤ－Ｒ記録モジュールを起動して、ＣＤ－Ｒライター１５に装填されているＣＤ－Ｒ１６に対して、上記電子透かしが埋め込まれたディジタルデータと共に自動インストールプログラム及び操作制御プログラムをＣＤ－Ｒ１６に書き込む。これにより、図４に示すように、電子透かしが埋め込まれたディジタルデータ３１、自動インストールプログラム３２及び操作制御プログラム３３が記録されたＣＤ－Ｒ１６が作成され、機密情報の記録処理が終了する。

【００６６】上記処理によって情報が記録されたＣＤ－Ｒ１６内のディジタルデータ３１は、上記の正規パスワードを知っている者だけが操作できるようになり、パスワードを知らない者は一切の操作を行うことができない。

【００６７】即ち、自動インストールプログラムは、これが書き込まれているＣＤ－Ｒ１６が情報再生装置のＣＤドライブ装置に装填されると自動的に起動して、操作制御プログラムを情報再生装置のメモリに常駐させて動作させる機能を有する。

【００６８】従って、ＣＤ－Ｒ１６を情報再生装置のＣＤドライブ装置に装填すると操作制御プログラムによる操作規制制御が行われる。

【００６９】例えば、コンピュータ本体１１のＣＤドライブ装置２６に上記の機密情報を記録したＣＤ－Ｒ１６を装填すると、自動インストールプログラム３２が自動的に起動して、操作制御プログラム３３をメモリ２２に常駐させて起動させる。

【００７０】操作制御プログラムが情報再生装置のメモリ内で動作を開始すると、ＣＰＵ２１は、ＣＤドライブ装置に装填されたＣＤに書き込まれているディジタルデータに対する情報記録再生装置からの操作を監視し、電子透かしデータが埋め込まれたデータに対する操作を規制する。

【００７１】この操作は、例えばディジタルデータのコピー操作、ディジタルデータが文字情報や画像情報である場合はその表示操作、ディジタルデータがコンピュータプログラムである場合にはその実行操作、ディジタルデータが音声情報である場合はその再生操作等である。

【００７２】即ち、図５に示すように、ＣＰＵ２１は、ＣＤ－Ｒ１６内のディジタルデータ３１に対する操作を監視し（ＳＢ１，ＳＢ２）、このディジタルデータ３１に対する操作が検出されると、この操作を中断させてパスワードの入力画面を表示する（ＳＢ３）。

【００７３】次いで、ＣＰＵ２１は、ディジタルデータ３１から正規パスワードを抽出して、操作者によって入力されたパスワードが正規パスワードであるか否かを判定する（ＳＢ４）。

【００７４】この判定の結果、入力されたパスワードが正規パスワードに一致しないときは上記中断していた操作を実行することなく終了させて（ＳＢ５）、後述するＳＢ７の処理に移行する。また、入力されたパスワードが正規パスワードに一致したときは、ＣＰＵ２１は、上記中断していた操作を実行する（ＳＢ６）。

【００７５】次に、ＣＰＵ２１は、ＣＤドライブ装置２６からＣＤ－Ｒ１６が取り出された否かを判定し（ＳＢ７）、取り出されていないときは上記ＳＢ１の処理に移行して前述の処理を繰り返し、ＣＤドライブ装置２６からＣＤ－Ｒ１６が取り出されたときは、上記の処理を終了して操作制御プログラム３３をメモリ２２から開放する。

【００７６】従って、ＣＤ－Ｒ１６に書き込まれているディジタルデータ３１は、パスワードを知っている者だけが操作することができる。パスワードを知らない者は、データのコピー、データの表示、プログラムの実行、データの音声再生等を行うことができない。これにより、ＣＤ－Ｒ１６に書き込まれているディジタルデータ３１の不正使用や改竄を防止することができる。

【００７７】尚、本実施形態では、正規パスワードを電子透かしデータの一部としてディジタルデータ３１に埋め込むようにしたが、操作制御プログラム３３内に埋め込むようにしても良い。また、これら双方を用いて異なる２つのパスワードをそれぞれに埋め込んで２重に規制するようにしても良い。

【００７８】次に、本発明の第２の実施形態を説明する。

【００７９】第２の実施形態では、第１の実施形態の構成に加えて、他のアプリケーションプログラムからＣＤ－Ｒ１６内のディジタルデータ１６を読み出して使用する場合に、ディジタルデータ３１から電子透かしデータを除去してからアプリケーションプログラムに引き渡す機能を、操作制御プログラム３３に設けた。

【００８０】即ち、コンピュータ本体１１のＣＤドライブ装置２６に上記の機密情報を記録したＣＤ－Ｒ１６が装填されて操作制御プログラム３３が起動されると、図６に示すように、ＣＰＵ２１は、ＣＤ－Ｒ１６内のディジタルデータ３１に対する操作を監視し（ＳＣ１，ＳＣ２）、このディジタルデータ３１に対する操作が検出されると、この操作を中断させてパスワードの入力画面を表示する（ＳＣ３）。

【００８１】次いで、ＣＰＵ２１は、ディジタルデータ３１から正規パスワードを抽出して、操作者によって入力されたパスワードが正規パスワードであるか否かを判定する（ＳＣ４）。

【００８２】この判定の結果、入力されたパスワードが正規パスワードに一致しないときは上記中断していた操作を実行することなく終了させて（ＳＣ５）、後述するＳＣ１１の処理に移行する。また、入力されたパスワードが正規パスワードに一致したときは、ＣＰＵ２１は、他のアプリケーションプログラムからのデータ読み出し操作であるか否かを判定する（ＳＣ６）。

【００８３】この判定の結果、他のアプリケーションプログラムからのデータ読み出し操作でないときは、上記中断していた操作を実行して（ＳＣ７）、後述するＳＣ１１の処理に移行する。また、他のアプリケーションプログラムからのデータ読み出し操作であるときは、ＣＤ－Ｒ１６からディジタルデータ３１を読み出して（ＳＣ８）、ディジタルデータ３１から電子透かしデータを除去したディジタルデータを生成し（ＳＣ９）、このディジタルデータを上記アプリケーションプログラムに引き渡す（ＳＣ１０）。

【００８４】次に、ＣＰＵ２１は、ＣＤドライブ装置２６からＣＤ－Ｒ１６が取り出された否かを判定し（ＳＣ１１）、取り出されていないときは上記ＳＣ１の処理に移行して前述の処理を繰り返し、ＣＤドライブ装置２６からＣＤ－Ｒ１６が取り出されたときは、上記の処理を終了して操作制御プログラム３３をメモリ２２から開放する。

【００８５】これにより、上記他のアプリケーションプログラムは、ディジタルデータ３１を電子透かしデータを除去した状態で使用することができる。従って、例えば目に見える電子透かしを用いた画像データを表示する場合にも、自動的に電子透かしが除去され、電子透かしのない画像データを表示させることができる。

【００８６】次に、本発明の第３の実施形態を説明する。

【００８７】第３の実施形態は、第２の実施形態の構成に加えて、ＣＤ－Ｒ１６へのデータ書き込みの際にディジタルデータ３１を暗号化するようにした。このための暗号モジュールはハードディスク装置２４に格納されている。

【００８８】第３の実施形態では、ＣＤ－Ｒ１６に機密情報を記録するために機密情報書き込みモジュールを起動すると、図７に示すように、ＣＰＵ２１は、まずパスワードの設定画面を表示してパスワードの設定を促す（ＳＤ１）。このパスワードは、前述と同様に操作者が任意に設定するもので、記録した情報を操作する際に使用するものである。

【００８９】次いで、ＣＰＵ２１は、記録対象となる情報のファイルの指定を促し、操作者によってファイルが指定されると、電子透かし埋め込みモジュールを起動して指定されたファイルのディジタルデータ（基本データ）に対して電子透かしデータを埋め込んだディジタルデータを生成する（ＳＤ２）。さらに、ＣＰＵ２１は、操作制御プログラム内に、前記ＳＤ１の処理で設定されたパスワードを正規パスワードとして埋め込んだ操作制御プログラム３３を生成する。

【００９０】この後、ＣＰＵ２１は、暗号モジュールを起動して、上記電子透かしデータが埋め込まれたディジタルデータを暗号化したディジタルデータを生成して（ＳＤ３）、ディジタルデータ３１とする。

【００９１】次に、ＣＤ－Ｒ記録モジュールを起動して、ＣＤ－Ｒライター１５に装填されているＣＤ－Ｒ１６に対して、上記電子透かしが埋め込まれさらに暗号化されたディジタルデータ３１と共に自動インストールプログラム３２及び正規パスワードを埋め込んだ操作制御プログラム３３をＣＤ－Ｒ１６に書き込む。

【００９２】これにより、機密情報の記録処理が終了する。

【００９３】一方、情報再生装置のＣＤドライブ装置に、例えばコンピュータ本体１１のＣＤドライブ装置２６に、上記の機密情報を記録したＣＤ－Ｒ１６が装填されて操作制御プログラム３３が起動すると、ＣＰＵ２１は次のように動作してディジタルデータ３１に対する操作規制を行う。

【００９４】即ち、図８に示すように、ＣＰＵ２１は、ＣＤ－Ｒ１６内のディジタルデータ３１に対する操作を監視し（ＳＥ１，ＳＥ２）、このディジタルデータ３１

に対する操作が検出されると、この操作を中断させてパスワードの入力画面を表示する（ＳＥ３）。

【００９５】次いで、ＣＰＵ２１は、ディジタルデータ３１から正規パスワードを抽出して、操作者によって入力されたパスワードが正規パスワードであるか否かを判定する（ＳＥ４）。

【００９６】この判定の結果、入力されたパスワードが正規パスワードに一致しないときは上記中断していた操作を実行することなく終了させて（ＳＥ５）、後述するＳＣ１１の処理に移行する。また、入力されたパスワードが正規パスワードに一致したときは、ＣＰＵ２１は、他のアプリケーションプログラムからのデータ読み出し操作であるか否かを判定する（ＳＥ６）。

【００９７】この判定の結果、他のアプリケーションプログラムからのデータ読み出し操作でないときは、上記中断していた操作を実行して（ＳＥ７）、後述するＳＥ１２の処理に移行する。また、他のアプリケーションプログラムからのデータ読み出し操作であるときは、ＣＤ－Ｒ１６からディジタルデータ３１を読み出して（ＳＥ８）、暗号モジュールを起動して復号を行う（ＳＥ９）。

【００９８】この復号処理においては、鍵（共通鍵或いは公開鍵）を必要とするため、鍵を持たない者は復号できない。

【００９９】次いで、ＣＰＵ２１は、復号が終了した暗号モジュールを開放し、復号したディジタルデータ３１から電子透かしデータを除去したディジタルデータを生成し（ＳＥ１０）、このディジタルデータを上記アプリケーションプログラムに引き渡す（ＳＥ１１）。

【０１００】次に、ＣＰＵ２１は、ＣＤドライブ装置２６からＣＤ－Ｒ１６が取り出された否かを判定し（ＳＥ１２）、取り出されていないときは上記ＳＥ１の処理に移行して前述の処理を繰り返し、ＣＤドライブ装置２６からＣＤ－Ｒ１６が取り出されたときは、上記の処理を終了して操作制御プログラム３３をメモリ２２から開放する。

【０１０１】このようにデータを暗号化することにより、機密保持機能をさらに向上させることができる。

【０１０２】尚、上記第１乃至第３の実施形態は、本発明の一具体例であって、本発明がこれらのみに限定されることはない。

【０１０３】また、上記各実施形態では、機密情報をＣＤ－Ｒ１６に書き込んで保存する場合に関して述べたが、これに限定されることはなく、第３者の不正使用を避けたい情報等であれば、同様に実施でき同様の効果が得られる。

【０１０４】また、上記各実施形態では、情報記録媒体としてＣＤ－Ｒ１６を用いたがこれに限定されることはない。しかし、ライトワンス追記型のＣＤ－Ｒを用いることによりデータの改竄防止効果は大きくなる。

【０１０５】また、上記各実施形態では、電子透かしデータを埋め込んだディジタルデータへの操作規制制御を行ったが、操作制御プログラムによって、電子透かしデータを埋め込んでいないディジタルデータへを含めて、ＣＤ－Ｒ１６に書き込まれた全てのデータ及びプログラムに対して操作規制するようにしても良い。

【０１０６】また、上記各実施形態では、情報の書き込みを行った情報機密保持システム１を用いて、情報が書き込まれたＣＤ－Ｒ１６に対するデータ操作を行った例を説明したが、他の情報再生装置等を用いても同様の効果が得られることが言うまでもないことである。

【０１０７】

【発明の効果】以上説明したように本発明の請求項１乃至請求項８記載の光情報記録媒体によれば、パスワードを知らない者は、書き込まれているディジタルデータへの操作を行うことができないので、前記ディジタルデータの不正使用や改竄を防止することができる。

【０１０８】また、請求項９乃至請求項１４記載の情報機密保持方法によれば、該方法によって情報が書き込まれた光情報記録媒体内の情報を操作するときに、パスワードを知らない者は、書き込まれているディジタルデータへの操作を行うことができないので、前記ディジタルデータの不正使用や改竄を防止することができる。

【０１０９】また、請求項１５乃至請求項２１記載の情報機密保持システムによれば、該システムの情報記録装置を用いて情報が書き込まれた光情報記録媒体内の情報を操作するときに、パスワードを知らない者は、書き込まれているディジタルデータへの操作を行うことができないので、前記ディジタルデータの不正使用や改竄を防止することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態における情報機密保持システムを示す外観図

【図２】本発明の第１の実施形態における情報機密保持システムの電気系回路示すブロック図

【図３】本発明の第１の実施形態における機密情報書き込み処理を説明するフローチャート

【図４】本発明の第１の実施形態における機密情報が書き込まれたＣＤ－Ｒを示す概念図

【図５】本発明の第１の実施形態における操作制御動作を説明するフローチャート

【図６】本発明の第２の実施形態における操作制御動作を説明するフローチャート

【図７】本発明の第３の実施形態における機密情報書き込み処理を説明するフローチャート

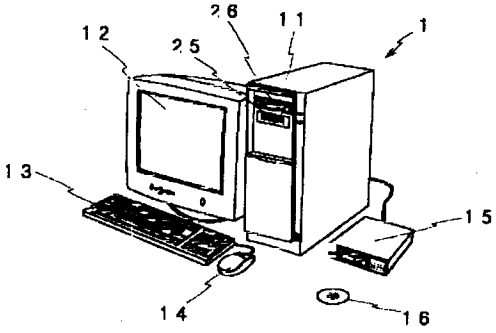
【図８】本発明の第３の実施形態における操作制御動作を説明するフローチャート

【符号の説明】

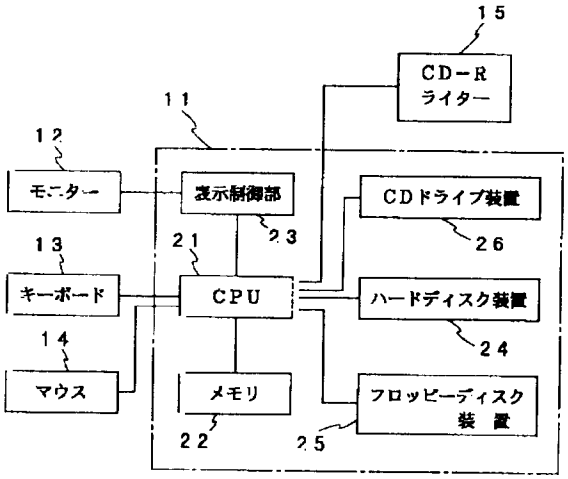
１…情報機密保持システム、１１…パーソナルコンピュータ本体、１２…モニター、１３…キーボード、１４…

マウス、15…CD-Rライター、16…CD-R、21…CPU、22…メモリ、23…表示制御部、24…ハードディスク装置、25…フロッピーディスク装置、26…CDドライブ装置、31…ディジタルデータ、32…自動インストールプログラム、33…操作制御プログラム。

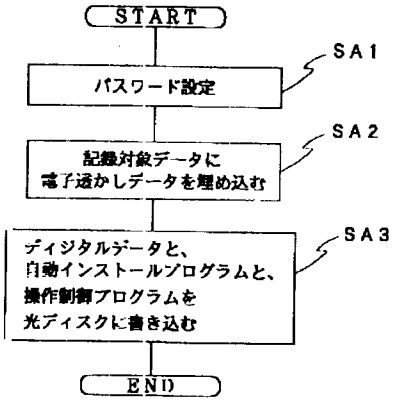
【図1】



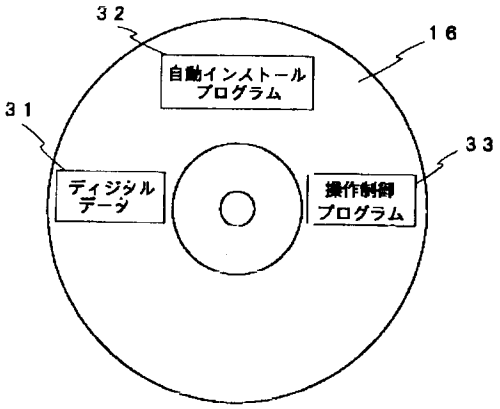
【図2】



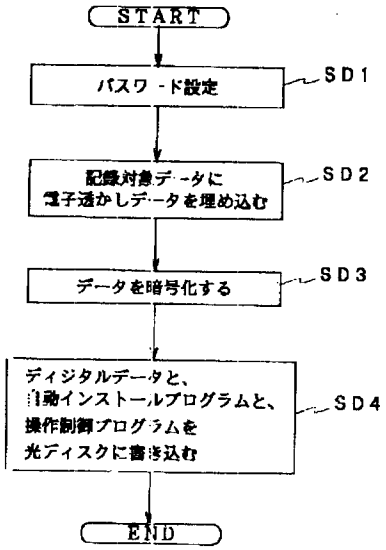
【図3】



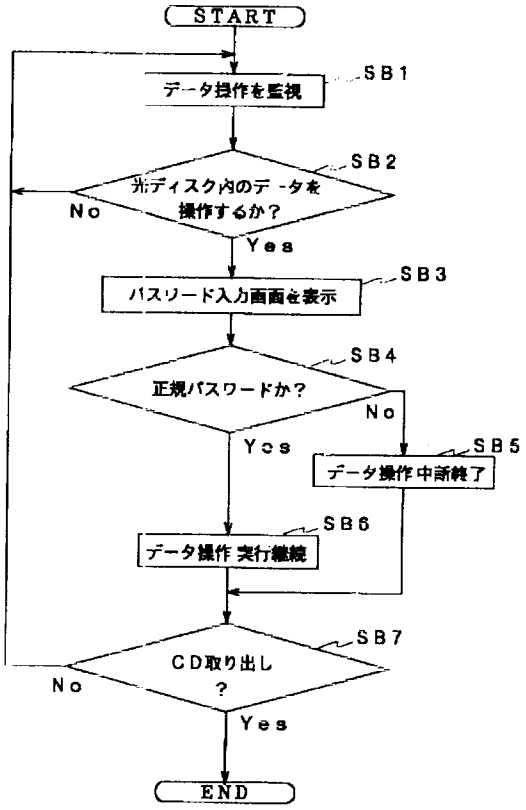
【図4】



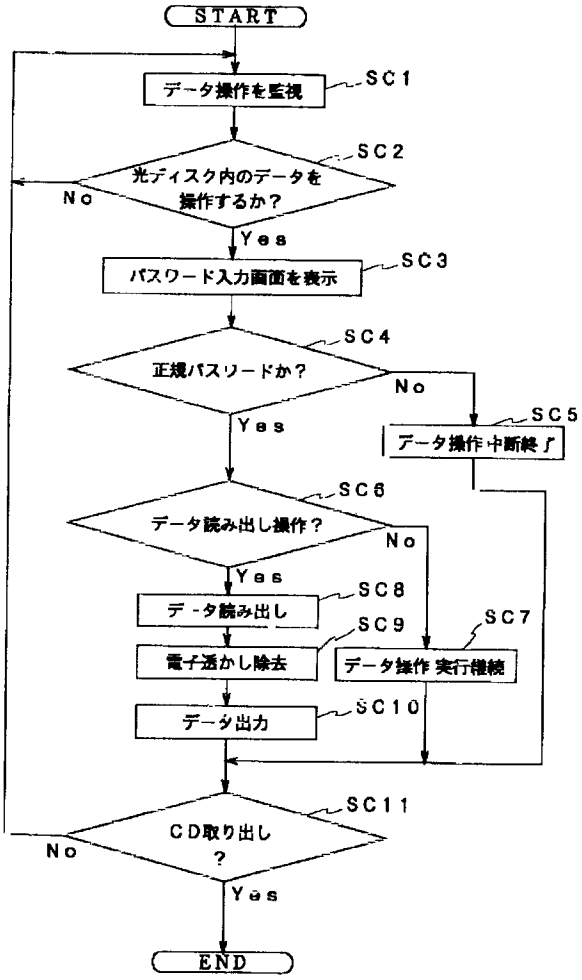
【図7】



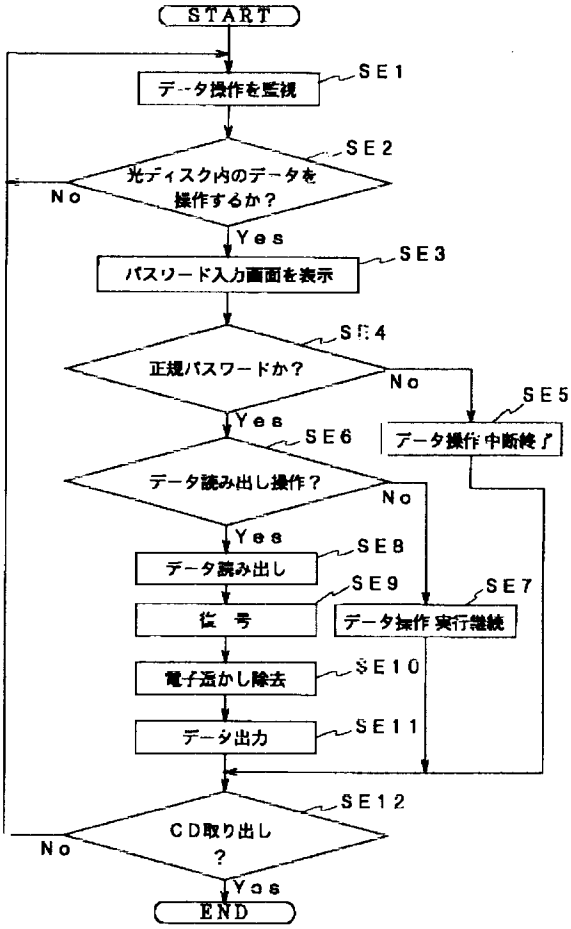
【図5】


START
データ操作を監視
SB1
光ディスク内のデータを操作するか？
SB2
No
Yes
パスワード入力画面を表示
SB3
正規パスワードか？
SB4
No
Yes
データ操作中断終了
SB5
データ操作 実行継続
SB6
CD取り出し？
SB7
No
Yes
END

【図6】


START
データ操作を監視
SC1
光ディスク内のデータを操作するか？
SC2
No
Yes
パスワード入力画面を表示
SC3
正規パスワードか？
SC4
No
Yes
データ操作中断終了
SC5
データ読み出し操作？
SC6
No
Yes
データ読み出し
SC8
電子透かし除去
SC9
データ操作 実行継続
SC7
データ出力
SC10
CD取り出し？
SC11
No
Yes
END

【図8】



フロントページの続き

Fターム(参考) 5B017 AA06 BA05 BA07 BB02 CA09
CA16
5D044 BC05 CC04 DE47 DE49 DE57
GK12 GK17
5J104 AA01 AA07 AA14 KA01 NA05
NA32 PA14
9A001 EE03 LL03